

**CLAIMS**

What is claimed is:

- 1    1. A method for preventing information losses due to  
2    network node failure, the method comprising the steps of:
  - 3       operatively connecting at least one backup node to a
  - 4       primary node;
  - 5       synchronizing the at least one backup node and the
  - 6       primary node;
  - 7       receiving, from a first endpoint, ingress traffic in
  - 8       the primary node;
  - 9       replicating the ingress traffic to the at least one
  - 10      backup node;
  - 11      outputting, from the primary mode, primary egress
  - 12      traffic;
  - 13      outputting, from the at least one backup node,
  - 14      backup egress traffic;
  - 15      determining if the primary node has failed;
  - 16      transmitting, to a second endpoint, the primary
  - 17      egress traffic if it is determined that the primary node
  - 18      has not failed; and
  - 19      transmitting, to the second endpoint, the backup
  - 20      egress traffic from a selected one of the at least one

21 backup nodes if it is determined that the primary node  
22 has failed,

23 wherein the backup egress traffic from the selected  
24 one of the at least one backup nodes replaces the primary  
25 egress traffic to the second endpoint and the backup node  
26 becomes the primary node for subsequent traffic.

1 2. The method of claim 1, wherein the primary node and  
2 the at least one backup node are network routers.

1 3. The method of claim 1, wherein the primary node and  
2 the at least one backup node are security engines for  
3 receiving encrypted ingress traffic and outputting  
4 decrypted egress traffic.

1 4. The method of claim 1, wherein the step of  
2 synchronizing the at least one backup node and the  
3 primary node further comprises the steps of:

4 transmitting synchronization information from the  
5 primary node to the at least one backup node.

1 5. The method of claim 4, wherein the step of  
2 transmitting synchronization information from the primary  
3 node to the at least one backup node further comprises  
4 the steps of:

5 transmitting at least one checkpoint message from  
6 the primary node to the at least one backup node, wherein

RECORDED MAILING RECEIPT

7 the at least one checkpoint message includes static  
8 information relating to the primary node as well as any  
9 outstanding session context for the primary node.

1 6. The method of claim 5, further comprising the steps  
2 of:

3 receiving, from the at least one backup node, a  
4 checkpoint message acknowledgment for each of said at  
5 least one checkpoint messages;

6 determining whether each of the checkpoint message  
7 acknowledgments were received prior to a change in flow  
8 state;

9 transmitting a synchronization declaration from the  
10 primary node to the at least one backup node if it is determined  
11 that each of the checkpoint message  
12 acknowledgments were received prior to a change in flow  
13 state; and

14 transmitting at least one new checkpoint message  
15 from the primary node to the backup node if it is determined  
16 that each of the checkpoint packet acknowledgments was  
17 not received prior to a change in flow state.

1 7. The method of claim 4, further comprising the steps  
2 of:

3       periodically assessing synchronization maintenance  
4   between the primary node and the at least one backup  
5   node.

6   8. The method of claim 7, wherein the step of  
7   periodically assessing synchronization maintenance  
8   further comprises the step of:

9           transmitting at least a portion of internal  
10   state information from the primary node to the at least  
11   one backup node sufficient to permit replication of  
12   primary node traffic on the at least one backup node.

1   9. An apparatus for preventing information losses due  
2   to network node failure, the apparatus comprising:

3       a primary node;

4       at least one backup node operatively connected to  
5   the primary node;

6       synchronizing means operatively connected to the  
7   primary node and the backup node for synchronizing the at  
8   least one backup node and the primary node;

9       means for receiving ingress traffic in the primary  
10   node from a first endpoint;

11       means for replicating the ingress traffic to the at  
12   least one backup node;

13       means for outputting primary egress traffic from the  
14      primary node;

15       means for outputting backup egress traffic from the  
16      at least one backup node;

17       determining means operatively connected to the  
18      primary node and the at least one backup node for  
19      determining whether the primary node has failed;

20       means for transmitting the primary egress traffic  
21      from the primary node to a second endpoint if the  
22      determining means determine that the primary node has not  
23      failed; and

24       means for transmitting the backup egress traffic  
25      from a selected one of the at least one backup nodes to  
26      the second endpoint if the determining means determine  
27      that the primary node has failed.

1      10. The apparatus of claim 9, wherein the primary node  
2      and the at least one backup node are network routers.

1      11. The apparatus of claim 9, wherein the primary node  
2      and the at least one backup node are security engines for  
3      receiving encrypted ingress traffic and outputting  
4      decrypted egress traffic.

1      12. The apparatus of claim 9, wherein the synchronizing  
2      means further comprise:

3       means for transmitting synchronization information  
4       from the primary node to the at least one backup node.

1     13. The apparatus of claim 12, wherein the means for  
2       transmitting synchronization information further  
3       comprise:

4       means for transmitting at least one checkpoint  
5       message from the primary node to the at least one backup  
6       node, wherein the at least one checkpoint message  
7       includes static information relating to the primary node  
8       as well as any outstanding session context for the  
9       primary node.

1     14. The apparatus of claim 13, further comprising:

2       means for receiving in the primary node, from the at  
3       least one backup node, a checkpoint message  
4       acknowledgment for each of said at least one checkpoint  
5       packets;

6       second determining means for determining whether  
7       each of the checkpoint message acknowledgments were  
8       received prior to a change in flow state;

9       means for transmitting a synchronization declaration  
10      from the primary node to the at least one backup node if  
11      is it determined that each of the checkpoint message

12 acknowledgments were received prior to a change in flow  
13 state; and

14 means for transmitting at least one new checkpoint  
15 message from the primary node to the backup node if it is  
16 determined that each of the checkpoint message  
17 acknowledgments was not received prior to a change in  
18 flow state.

1 15. The apparatus of claim 12, further comprising:

2 means for periodically assessing synchronization  
3 maintenance between the primary node and the at least one  
4 backup node.

5 16. The apparatus of claim 15, wherein the means for  
6 periodically assessing synchronization maintenance  
7 further comprise:

8  
9 means for transmitting at least a portion of an  
10 internal state of the primary node to the backup node  
11 sufficient to permit replication of primary node traffic  
12 on the at least one backup node..

1 17. An article of manufacture for preventing information  
2 losses due to network node failure, the article of  
3 manufacture comprising:

4 at least one processor readable carrier; and

DRAFTING STYLING SHEET  
1. LINES: 1/2" HORIZONTAL, 1/4" VERTICAL  
2. SPACING: 1/4" LINE, 1/2" PARAGRAPH  
3. LETTERS: 10 PT. 45° ANGLED  
4. NUMBERS: 10 PT. 45° ANGLED  
5. TABLES: 10 PT. 45° ANGLED  
6. FIGURES: 10 PT. 45° ANGLED  
7. CANCELLATION: 10 PT. 45° ANGLED  
8. FONTS: HELVETICA, 10 PT.

5       instructions carried on the at least one carrier;  
6       wherein the instructions are configured to be  
7       readable from the at least one carrier by at least one  
8       processor and thereby cause the at least one processor to  
9       operate so as to:

10      synchronize a primary node and at least one  
11     operatively connected backup node;

12      receive, from a first endpoint, ingress traffic;

13      replicate the ingress traffic to the at least one  
14     backup node;

15      output, from the primary node, primary .. egress  
16     traffic related to the ingress traffic;

17      output, from the at least one backup node, backup  
18     egress traffic related to the ingress traffic;

19      determine if the primary node has failed;

20      transmit, from the primary node, primary egress  
21     traffic related to the ingress traffic to a second  
22     endpoint if it is determined that the primary node has  
23     not failed; and

24      transmit, from a selected one of the at least one  
25     backup nodes, backup egress traffic to the second  
26     endpoint if it is determined that the primary node has  
27     failed,

28       wherein the backup egress traffic replaces the  
29 primary egress traffic to the second endpoint and the  
30 selected one of the at least one backup nodes becomes the  
31 primary node for subsequent traffic.

1       18. The article of manufacture of claim 17, wherein the  
2 instructions further cause the at least one processor to  
3 operate so as to:

4       transmit synchronization information from the  
5 primary node to the at least one backup node.

1       19. The article of manufacture of claim 18, wherein the  
2 instructions further cause the at least one processor to  
3 operate so as to:

4       transmit at least one checkpoint message from the  
5 primary node to the at least one backup node, wherein the  
6 at least one checkpoint message includes static  
7 information relating to the primary node as well as any  
8 outstanding session context for the primary node.

1       20. The article of manufacture of claim 19, wherein the  
2 instructions further cause the at least one processor to  
3 operate so as to:

4       receive, from the at least one backup node, a  
5 checkpoint message acknowledgment for each of said at  
6 least one checkpoint messages;

7       determine whether each of the checkpoint message  
8    acknowledgments were received prior to a change in flow  
9    state;

10      transmit a synchronization declaration from the  
11     primary node to the at least one backup node if is it  
12     determined that each of the checkpoint message  
13     acknowledgments were received prior to a change in flow  
14     state; and

15      transmit at least one new checkpoint message from  
16     the primary node to the backup node if is determined that  
17     each of the checkpoint message acknowledgments was not  
18     received prior to a change in flow state.

1    21. The article of manufacture of claim 18, wherein the  
2    instructions further cause the at least one processor to  
3    operate so as to:

4       periodically assess synchronization maintenance  
5    between the primary node and the at least one backup  
6    node.

1    22. A computer data signal embodied in a carrier wave  
2    readable by a computing system and encoding a computer  
3    program of instructions for executing a computer process  
4    performing the method recited in claim 1.